通信情報保護學會誌
第5卷 第4號, 1995. 12

논리적 보안 통제

Logical Security Control

최 운 식*, 신 동 익*

요 약

본 연구는 보안 통제를 물리적, 논리적, 관리적 통제로 구분하고, 그 중에서 시스템에 논리적으로 구현되는 논리적 통제에 중점을 두고 있다. 최근 정보기술과 통신의 급격한 발달과 접목은 정보시스템을 새로이 취약성에 노출시키고 있으며, 이에 대응하기 위하여 논리적 통제의 중요성이 점점 부각되고 있다. 본 연구는 논리적 통제 중에서 모든 종류의 시스템에 필수적으로 필요한 통제로 인증, 접근통제, 감사로 그 세가지를 들고, 이 세가지 통제에 대한 상호관계를 규정하는 체계와 각각의 통제에 대한 설명을 한다.

1. 서 론

네트워크의 확산은 원거리의 사용자가 멀리서도 컴퓨터 시스템을 접근하여 손쉽게 정보를 교환하거나 업무를 처리할 수 있게 하여 수많은 이익을 제공하고 있으나, 소프트웨어나 자료의 보안 측면에서는 많은 문제점을 제기하고 있다. 즉 정보시스템이 통신망으로 서로 연결됨에 따라 단순한 물리적 보안만으로는 시스템의 보안성을 유지하기 어렵게 되었다. 보다 완벽한 보안성 유지를 위해서는 논리적 보안 통제를 시스템내에 구현하여야 한다. 논리적 보안 통제는 시스템의 물리적 측면과 대응하여 논리적 측면을 강조한다. 즉 시스템 내부에 보안 통제를 담당하는 보안 서비스를 논리적으로 구현하는 것을 말한다. 본 연구는 논리적 보안 통제에서 시스템의 종류에 상관없이 필수적으로 필요한 논리적 보안 통제를 식별하고, 이 통제들을 최근의 연구 결과와 함께 설명한다.

흔히 보안 관련 문헌은 보안 정책, 보안 통제, 보안 서비스 등이 혼재되어 사용되고 있다. 여러 종류의 해석이 있을 수 있겠으나, 본 연구에서는 보안 정책은 최고경영자가 제시하는 그 조직의 전반적인 보안에 대한 방향을 의미를 하며, 보안 통제는 보안 정책을 실현하기 위해 필요한 통제를 의미한다. 보안 통제에는 여러종류가 있을 수 있으며, 또한 구분하는 방법이 다양하다. 본 연구는 가장 많이 사용하고 있는 물리적, 논리적, 관리적 통제의 구분을 사용하고자 한다.

최근 급격한 정보기술과 통신의 발달과 접목은 논리적 보안 통제의 중요성을 부각시켰

* 한국전산원

으며, 특히 새로운 논리적 보안 통제의 개발을 촉진시키고 있다. 흔히 논리적 보안 통제는 보안 서비스라고도 불리우며, 보안 서비스는 다양한 종류의 보안 메카니즘을 선택 또는 종합하여 실현된다. 보안 서비스와 보안 메카니즘과의 관계는 국제표준인 ISO 7498-2에 잘 설명되어 있으며, 최근 더욱 다양한 보안 서비스와 메카니즘, 그리고 메카니즘을 구현하는 알고리즘에 대한 연구가 진행되고 있다[1].

ISO 7498-2는 보안 서비스로서 인증(authentication), 접근통제(access control), 자료 비밀성(data confidentiality), 자료 무결성 (data integrity), 부인봉쇄(nonrepudiation)의 5가지를 들고 있다. 이중에서 시스템의 목적과 종류에 상관없이 기본적으로 필요한 서비스는 인증과 접근통제라 하겠다. 인증과 접근통제는 전통적으로 많이 사용되어 왔으며, 최근에 와서도 그 중요성은 줄어들지 않고 있다. 인증과 접근통제 이외에 시스템의 관리자 입장에서 중요한 통제는 감사이다. 감사는 감사로그를 분석하여 그 결과를 보안사고의 예방에 힘쓰는 것이다. 따라서 사후적인 측면의 보안통제이나, 보안 감사 도구가 소프트웨어로 구현되어 사용되고 있으며, 경우에 따라서는 실시간으로 작동하여 침입탐지를 하는 데에도 사용된다. 감사라는 보안통제가 논리적 통제로 자리를 잡고 있음을 알 수 있다.

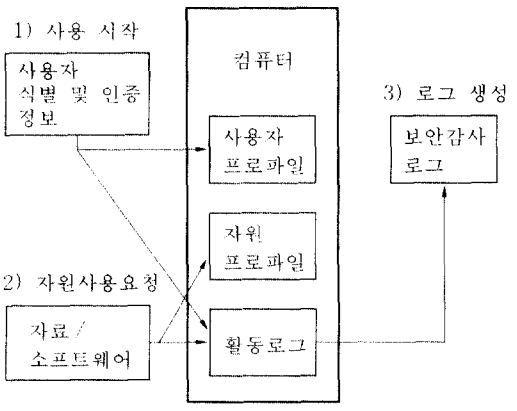
본 연구에서는 논리적 보안 통제를 아래와 같이 크게 세가지로 구분하여 살펴보고자 한다. 아래의 세가지 통제는 이 통제들이 충분하다는 것을 의미하지는 않는다. 다만 아래의 세가지 통제는 시스템의 종류와 상관없이 필수적으로 필요한 통제라는 것이다.

- 사용자 식별(identification) 및 인증(authentication)
- 자원 사용 접근 통제
- 감사 로그(audit log)

일반적으로 식별을 위해서는 사용자 식별자(user-iD)가 사용되며, 인증을 위해서는 패스워드 시스템이 많이 사용된다. 또다른 방법으로 토큰(token)이나, 생체측정(biometrics) 방법이 사용되기도 한다. 최근 EDI와 같은 시스템의 활발한 구축은 전자서류의 사용을 급격히 활성화시켰으며, 따라서 전자서류의 보호와 인증에 사용되는 전자서명(digital signature) 또한 중요시 되고 있다.

자료나 소프트웨어에 대해 사용자의 접근을 제한하는 접근 통제로는 임의적 접근 통제(discretionary access control)와 강제적 접근 통제(mandatory access control), 역할에 따른 접근 통제(role-based access control) 등이 있다.

마지막으로 고려되어야 할 통제는 사용자가 부여된 권한을 갖고 자원을 사용하여 여러가지 활동을 한 행적에 대한 로그(log)를 생성하여 보안 감사추적을 가능토록하는 것이다. 다중사용자 시스템에서 보안감사 로그는 필수적이며, 이를 이용해서 의심스러운 활동을 경고 및 적발하고, 컴퓨터 범죄나 오용시에는 증거자료로 사용할 수도 있다.



〈그림 1〉 논리적 보안통제의 개관

〈그림 1〉은 위의 세가지 논리적 보안 통제의 관계를 보여주고 있다. 사용시작(log-on)은 사용자가 시스템 사용을 위해 접근하는 것을 말하며, 여기서 주요활동은 사용자의 식별 및 인증이다. 컴퓨터 시스템은 사용자 프로파일을 이용하여, 사용자를 식별하고 인증한다. 접근이 허락된 사용자는 필요한 자료나 프로그램의 사용을 요청하며, 사용자의 기원 사용 권한에 따라 접근 가능여부가 결정된다. 사용자의 접근 시도 및 접근 후의 활동은 로그 파일에 기록되어 보안감사를 위한 증거로 사용된다.

2. 사용자 식별(identification) 및 인증(authentication)

통계적으로 볼 때, 대부분의 컴퓨터 관련 범죄는 컴퓨터와 관련된 업무에 종사하는 내부 사용자에 의해 발생하고 있다. 그러나 네트워크가 확산됨에 따라 외부 사용자에 의한 시스템 침입도 증가하고 있다. 허가되지 않은 사용자의 접근을 막고, 정보를 안전하게 보호하기 위해서는 컴퓨터 시스템에 접근하는 사용자의 식별 및 인증이 매우 중요하다.

사용자 식별 및 인증 방법은 크게 세가지 형태로 분류할 수 있다.

첫째, 사용자가 알고 있는 것(패스워드)을 이용한 식별 및 인증

둘째, 사용자가 소유하고 있는 것(토큰)을 이용한 식별자 및 인증

세째, 사용자가 신체의 일부(생체측정)를 이용한 식별자 및 인증

2.1 패스워드 시스템

패스워드 시스템은 가장 널리 이용되는 사용자 식별 및 인증 방법이다. 패스워드는 문자, 숫자, 특수기호 등으로 구성되며, 사용자 식별자(ID)와 상호 연결되어 있다. 사용자는 시스템에 접근하기 위해 자신의 ID와 패스워드를 입력한다. 시스템은 입력된 사용자 식별자와 패스워드를 시스템에 저장된 식별자 및 패스워드와 비교하여 일치할 경우, 사용자의 접근을 허용한다.

사용자 식별자는 공개되어 있으나, 패스워드는 비밀성이 유지되어야 한다. 추측이 용이하거나 길이가 짧은 패스워드는 외부 시스템 침입자에 의해 쉽게 노출될 수 있으므로 좋은 패스워드가 될 수 없다. 좋은 패스워드가 되기 위해서는 아래의 조건들을 갖추어야 한다.

① 문자와 숫자, 특수기호 등을 함께 사용하며, 기억하기 쉬워야 한다.

패스워드 문자의 조합 가능한 갯수는 X^y이다. 여기서 X는 패스워드에 사용될 수 있는 모든 문자나 숫자, 기호의 총 갯수이며, y는 패스워드의 길이이다. 따라서 X가 클수록 조합 가능한 패스워드의 갯수가 증가하므로 패스워드 추측이 어렵게 된다. 그러나 "!r$*+3@"와 같은 패스워드는 오히려 기억하기가 어려우므로 패스워드를 따로 적어둘 위험이 있다.

② 일정 길이 이상 유지되어야 한다.

패스워드의 길이를 나타내는 y의 값이 클수록 패스워드의 조합 가능한 갯수는 증가하며, 추측에 의한 패스워드 공격에 보다 안전할 수 있다. 따라서 패스워드를 일정 길이 이상 유지하여야 한다.

③ 패스워드는 주기적으로 교환하여야 한다.

패스워드는 주기적으로 바꾸어야 하며, 노출되었다고 의심이 될 때에는 즉시 바꾸어야 한다. 새로운 패스워드는 기존의 N개까지의 패스워드와 다를 때에만 받아들이게 하여야 한다. 또한 수명이 다한 패스워드는 자동으로 바꾸게 하는 기능이 있어야 한다.

일반적으로 많이 사용되고 있는 패스워드 시스템으로는 아래 세가지 유형이 있다.

- 일정기간 사용 패스워드(long term passward)
- 일회용 패스워드(one time passward)
- 암호구(pass phrase)

- 일정기간 사용 패스워드(long term passward) : 일반적으로 가장 널리 사용되는 패스워드 시스템으로 동일한 패스워드를 일정기간 동안 여러번 사용할 수 있으며, 주기적으로 변경하여야 한다. 그러나 크랙(crack)이나 스니프(sinffer)와 같은 패스워드 해독 프로그램에 의해 암호가 노출될 가능성이 많다.

- 일회용 패스워드(one time passward) : 일회용 패스워드 시스템이란 시스템에 접근할 때마다 새로운 패스워드를 요구하는 시스템을 말한다. 시스템과 사용자가 동일한 함수를 이용하여 매번 새로운 패스워드를 생성하는 것이다. 사용자는 자신의 패스워드 생성 함수를 알고 있거나, 패스워드를 자동으로 계산해 주는 장치를 갖고 있어야 한다. 아래에 간단한 일회용 패스워드 생성 함수의 예를 설명하였다.

. f(x) = x + 1. 사용자가 시스템에 접근시 지난 패스워드 x가 나타나며, 사용자는 x + 1을 계산하여 새로운 패스워드로 입력한다. 이때 함수 f(x)는 사용자만 알고 있어야 한다. 다른 예로 f(x) = d * h가 사용될 수도 있다. 여기서 d는 현재 날짜이며, h는 현재 시간이다.

. f(x) = r(x). 사용자는 최초의 무작위 수(random number) x를 자신의 패스워드 계산 장치에 입력한다. 함수 r(x)는 무작위 수를 x개 계산하여, x번째 무작위 수를 최종 결과로 산출한다. 시스템에 접근시 사용자는 무작위수 x와 r(x)의 결과 값을 함께 입력한다. 이때 함수 r(x)는 사용자마다 달라야 한다.

. f(E(x)) = E(D(E(x)) + 1). 시스템은 사용자에게 암호화된 값 E(x)를 보낸다. 사용자는 E(x)를 복호화하여 D(E(x)) + 1을 계산 후, 계산 결과를 암호화하여 패스워드로 입력한다.

이상은 일회용 패스워드 생성 함수를 간단히 설명할 수 있는 일례를 든 것이며, 실제로는 매우 복잡한 함수가 사용된다. 일회용 패스워드 시스템은 보안성이 매우 뛰어나며, 크랙(crack)이나 스니프(sinffer) 같은 해독 프로그램에 의해 암호가 노출될 위험이 없다. 그러나 사용자들이 패스워드 생성함수를 기억해야 하는 어려움과 패스워드 생성 장치를 분실할 위험이 있다.

- 암호구(pass phrase) : 암호구란 문장 길이의 패스워드를 말한다. 즉, 사용자가 쉽게 기억할 수 있는 문장을 하나의 패스워드로 사용하는 것이다. 예를 들어, 노래가사의 한 귀절이나, 자신만이 알고 있는 하나의 문장 등이 암호구로 사용될 수 있다. 암호구의 사용은 메모리를 많이 사용하는 단점이 있으나, 암호화 된 암호구의 특정 부분만 패스워드로 저장하거나, 암호문을 암축하는 방법 등으로 이를 해결할 수 있다.

2.2 토큰

토큰이란 사용자가 자신의 신분을 확인 받기 위해 사용하는 물체를 말한다. 여러 분야에서 자신의 인증을 위해 ID 카드가 많이 사용되고 있다. ID카드가 효력을 발생하기 위해서는 위조가 불가능하여야 하며, 유일무이하여야 한다.

자기 테이프 카드는 널리 이용되고 있는 토큰의 한 형태이다. 자기 테이프 카드의 가장 일반적인 사용예는 은행에서 발급되는 신용카드의 경우이다. 신용카드 소지자는 24시간 어느때나 현금을 인출할 수 있다.

그러나 카드만으로는 완벽한 신분 인증이 불가능하며, 비밀번호가 필요하다.

또한 다른 형태는 스마트 카드나 칩 카드이다. 스마트 카드나 칩카드는 카드내에 자기 테이프 대신 반도체 칩이 내장되어 있다. 스마트 카드에는 카드 소유자의 신분 정보가 저장되어 있을 뿐만 아니라 간단한 계산이나, 암호화를 수행할 수 있는 기능도 있다.

예를 들어 사용자가 시스템에 접근하고자 할 경우, 스마트 카드 입력기에 자신의 스마트 카드를 입력 후, 자신의 ID와 패스워드를 타이핑하면 스마트 카드에서 입력된 패스워드를 암호화하여 시스템에 입력한다. 따라서 라인태핑(line tapping) 등에 의해 패스워드가 노출될 위험을 방지할 수 있다.

토큰 사용의 단점은 사용자가 토큰을 분실하거나, 현재 갖고 있지 않을 경우, 시스템 사용이 불가능하며, 분실된 토큰이 제3자에 의해 사용될 경우, 토큰 소유자에게 큰 피해를 줄 수 있다는 것이다.

2.3 생체 측정

또 다른 인증 방법은 지문, 음성, 망막의 형태, 서명 동작 등 사용자의 신체적 특성, 즉 생체 측정을 이용하는 것이다. 지문이나, 음성 등은 분실되거나 위조될 가능성이 낮으므로 안전하며, 신뢰성이 매우 높은 매체가 될 수 있다. 생체 측정초기 단계에서는 부당한 거부(false rejection)가 발생할 가능성이 높으나, 통계적으로 볼 때, 측정 횟수가 증가할 수록 부당한 거부가 발생할 가능성은 감소한다[3].

2.3.1 서명 검증(signature verifier)

서명 검증 장치는 시스템에 서명 판을 갖추고 있으며, 사용자는 서명판에 자신의 서명을 한다. 서명 검증 장치는 서명시 펜의 압력, 서명 속도, 서명 형태 등을 분석하여 측정치가 오차 허용 범위를 벗어나지 않으면 접근을 허용하게 된다. 평균적으로 서명 검증에서 부당한 거부가 발생한 가능성은 2% 수준이다.

서명 검증 장치의 단점은 사용자 편의성이 낮은 것이다. 최초 시스템에 자신의 서명 정보를 입력하기 위해 서명판에 수십번 서명을 하여야 하며, 서명시에는 서명 속도와 펜의 압력에 항상 주의하여야 한다.

2.3.2 망막 측정

망막 측정 방법은 망막에 있는 실핏줄의 형태를 측정하여 사용자의 신분을 인증하는 것이다. 눈의 망막은 사람마다 고유하며, 쉽게 변하지 않는 특성을 가지고 있다.

망막 측정 장치는 약한 적외선 레이저 빔을 이용하여 망막의 실핏줄을 읽어 들인다.

이 방법은 오류률이 매우 낮으며, 허가되지 않은 사용자의 접근을 완벽히 막을 수 있다.

그러나 망막 측정 방법의 단점은 망막 측정 장치에 대해 사용자가 거부감을 느낄 수 있다는 것이다. 비슷한 방법으로 눈의 홍채(虹彩)를 측정하는 장치가 있다. 이 장치는 약간 떨어진 거리에서도 측정이 가능하므로 사용자의 거부감을 줄일 수 있다는 장점이 있다.

2.3.3 지문 측정

지문은 잘 변화지 않으며, 사람마다 다르기 때문에 19세기 후반부터 인증 기법으로 사용되어 왔다. 지문 측정 장치는 지문의 모양, 끝점의 위치, 각도 등을 읽은 후, 시스템에 저장된 지문 정보와 비교하여 사용자를 식별 및 인증한다. 지문의 측정 각도가 조금 다르거나, 지문에 상처가 생겼을경우, 시스템에 저장된 지문 정보와 오차가 발생할 수 있으며, 지문 측정에 어려움이 있을 수 있다. 또한 손이 얼어 있거나, 사용자가 고령인 경우에도 부당한 거부가 발생할 가능성이 높다.

2.3.4 음성 측정

음성 측정 방법은 특정 단어나 구에 대한 사용자의 음성을 디지탈화하여 시스템에 저장한 후, 시스템 접근시 특정 단어나 구에 대한 사용자의 실제 음성과 비교하는 것이다.

음성 측정은 사용자의 생리적 특징이나 행위적 특징들을 조합하여 이루어지므로 모방이 어렵다. 그러나 음성 측정 장치 주변에 소음이 심하거나, 사용자의 건강상태에 의해 목소리가 달라졌을 경우, 정확한 측정을 할 수 없는 단점이 있다.

3. 자원 사용 접근 통제

접근 통제 규칙을 수립시에는 개인별로 접근 권한을 부여하는 것보다 역할이나 지위에 따라 접근 권한을 부여하는 것이 더욱 효과적이며, 간단하다. 접근 권한을 결정하는 것은 많은 주의와 시간이 요구되는 작업이다. 사용자 그룹을 정의하고 각 그룹의 작업 내용과 필요로 하는 정보, 각 그룹에서 생산되는 정보, 사용하는 장비, 각 그룹이 요구하는 접근 권한 수준 등을 신중히 고려하여 접근 권한을 부여하여야 한다.

3.1 자원 접근 통제 개요

자원에 대한 접근 통제는 접근 통제 방침의 수립과 접근 통제 메카니즘의 개발로 구현될 수 있다. 이 절에서는 접근통제 방침에 대해 언급할 것이다.

TCSEC에서 접근 통제 유형을 임의적 접근통제(discretionary acess control)와 강제적 접근통제(mandatory access control) 두가지로 구분하고 있다. 이 절에서는 두가지 접근통제외에 역할에 따른 접근통제(roll-based access control)도 포함하였다. 세가지 접근통제가 사용되는 경우를 보면, 강제적 접근통제는주로 보안 등급이 명확히 구분되는 군사 정보에 적용되며, 임의적 접근 통제는 행정이나 상업 정보에 적용된다. 역할에 따른 접근통제는 임의적 접근통제보다 행정이나 상업정보에 더 적합한 것으로 평가받고 있다.

임의적 접근 통제는 시스템 사용자가 자신의 통제하에 있는 자원에 대해 다른 사용자가 접근하는 것을 임의로 허가하거나 허가하지 않을 수 있는 방법이다. 이것은 사용자 식별자나 사용자 그룹 식별자에 따라 자원에 대한 접근을 통제하는 것으로 자원에 대한 접근 통제 권한을 가진 사용자가 시스템 관리자의 승인없이 접근 권한을 다른 사용자에게 임의로 부여해줄 수 있다. 그러나 대부분의 경우, 최종 사용자는 임의로 접근을 통제할 수 있는 자원을 소유하지 않고 있다.

많은 조직에서 자원에 대한 접근은 사용자의 역할과 지위에 의해 결정된다. 여기에는 사용자의 임무, 책임, 능력 등이 포함된다. 역할에 따른 접근통제는 조직내에서 사용자들이 수행하는 역할에 따라 자원에 대한 접근을 통제하는 방법이다. 이 경우 사용자들은 자신의 재량으로 다른 사용자에게 접근 권한을 부여할 수 없으므로 임의적 접근통제 방법과는 다르다.

접근 권한의 부여는 시스템 관리자의 임의적 재량보다는 조직의 시스템 보안 방침에 따라 결정된다. 보안 방침은 조직의 법이나 윤리 조항, 규칙, 통제 등에서 반영된다. 보안 방침은 모든 사용자에게 예외없이 적용되므로 비임의적(nondiscretionary)이라고 말할 수 있다. 의사의 경우를 예를 들면, 의사는 환자에게 약을 처방할 수는 있으나, 약을 처방할 수 있는 권한을 간호원에게 이양할 수는 없다.

역할에 따른 접근통제는 사실상 강제적 접근통제의 형태를 띄고 있으나, 자원의 보안 등급에 따라 접근을 통제하지 않는다는 점에서 강제적 접근통제와는 다르다.

강제적 접근통제는 자원의 민감도에 따라 보안 등급을 분류하고, 보안 등급별로 사용자에게 접근 권한을 부여하는 것이다. 강제적 접근 통제 방침에서는 "누가 어떤 정보를 읽을 수 있는냐?" 하는 것을 중요시 한다. 보안등급이 높은 정보가 보안 등급이 낮은 곳으로 이동하는 것은 엄격히 통제된다. 역할에 따른 접근 통제 방침은 "누가 어떤 정보에 어떤 활동을 할 수 있는가?"를 중요시 한다. 이장에서는 역할에 따른 접근 통제를 중심적으로 언급하겠다.

3.2 역할에 따른 접근 통제(role-based access control)[5,6,7]

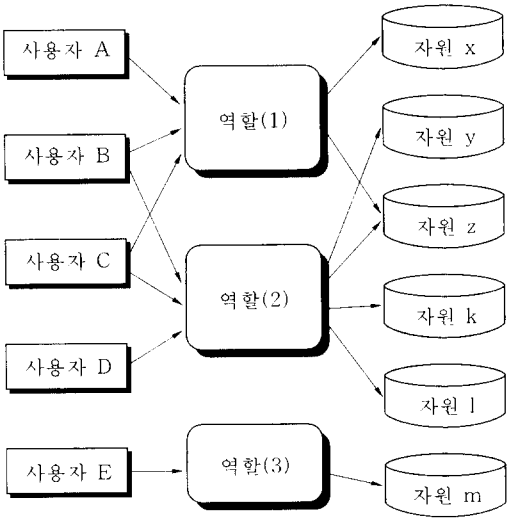
임의적 접근통제는 정보 자산의 효과적인 보호 및 관리상에 취약점이 많으며, 강제적 접근 통제는 보안 등급이 분류된 정보에 한정되는 단점이 있다. 이러한 단점을 극복하고 정보 자산을 효과적으로 보호하고 관리할 수 있는 방법으로 역할에 따른 접근 통제가 많이 사용되고 있다.

역할에 따른 접그 통제는 세가지 조건이 갖추어져야 한다.

첫째, 모든 사용자는 자신에게 역할이 주어졌을 때에만 활당된 자원을 사용할 수 있어야 한다. 둘째, 사용자는 허가된 역할만 수행하여야 한다.

세째, 사용자는 자원이 자신에 허가될 경우에만 사용할 수 있어야 한다.

위의 세가지 조건에 의해 사용자는 자신에게 역할이 명확히 주어지고, 역할에 의해 사용이 허가된 자료에만 접근할 수 있다. 역할에 따른 접근 통제 방법의 장점은 특정 역할을 부여받은 사용자에게 허용될 수 있는 자원을 논리적으로 구분할 수 있다는 것이다. 역할에 따라 필요한 자원의 할당이 완료되면, 사용자는 자신에게 주어진 역할을 수행하기 위해 할당된 자원을 사용할 수 있다. 역할에 따라 접근 가능한 자원들이 이미 결정되어 있으므로 특정 사용자에게 어떤 자원이 필요한지 따로 결정할 필요가 없다. 〈그림 2〉는 사용자의 역할에 따른 자원 접근 관계를 보여주고 있다. 사용자는 하나 이상의 역할을 부여 받을 수 있으며, 하나의 역할에 다수의 사용자가 포함될 수 있다. 사용자가 접근할 수 있는 자원은 사용자에게 부여된 역할에 의해 결정된다. 사용자의 역할이 변경될 경우, 사용자와 역할사이의 연결고리(화살표)를 조정하므로 사용자의 접근 권한을 쉽게 변경할 수 있다.



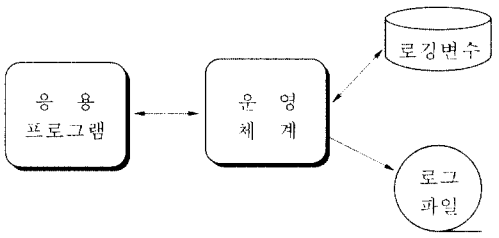
〈그림 2〉 역할에 따른 자원 접근 관계

4. 보안감사 로그

보안 감사 로그는 시스템에 일어난 모든 활동을 시간 순서별로 기록해 두는 것이다. 감사 로그는 시스템의 허가되지 않은 사용을 방지하고, 문제 해결을 위한 정보 제공할 수 있으며, 시스템 모니터링을 가능케 해준다.

대부분의 운영 체계는 시스템에 일어난 모든 활동에 대한 로깅 기능을 제공해 줄 수 있다. 사용자는 시스템내에 모든 응용 프로그램

에 대해 어떠한 데이타를 로그해야 하는지 결정하여 운영체계내에 시스템 변수로 입력해 두면 응용 프로그램이 실행 될 때마다 운영체계는 지정된 변수에 따라 필요한 정보를 로깅해 준다. 〈그림 3〉에 운영 체계에 의한 감사 로그 생성 절차를 나타내었다.



〈그림 3〉 운영 체계에 의한 감사 로그 생성 절차

일반적으로 네가지 형태의 로그 파일이 존재한다.

첫번째 형태는 자원 사용과 관련된 로그 파일이다. 여기에는 자원을 사용한 사용자, 응용 프로그램, 사용 시간 등의 정보가 기록된다. 자원 사용과 관련된 로그 파일은 일반적으로 자원 관리와 감사 목적으로 사용된다. 감사 목적 이외에 시스템 사용료 청구나, 시스템 성능을 평가하기 위한 자료로 사용될 수도 있다. 즉, 하나의 데이타를 처리하는데 소요되는 시간을 계산하거나, 시스템 병목 현상의 원인을 찾기 위한 자료로 사용될 수 있다. 시스템 성능 평가를 통해 프로그램을 수정하거나, 시스템을 효율적으로 재구성 할 수 있다. 또한 허가되지 않은 시스템 사용을 방지할 수 있다. 일반적으로 시스템이 언제, 누구에 의해 얼마나 자주 사용되었는지를 파악해 둠으로서 예외적인 사항이 발생할 경우, 허가되지 않은 시스템 사용 가능성을 추적할 수 있다.

두번째 형태는 의도적인 무결성 침해와 관련된 로그 파일이다. 성공하지 못한 자원 접근 시도를 로그 파일에 기록해 두는 것이다. 예를 들어 허가되지 않은 자원에 접근하려고 하였을 경우, 이러한 시도를 로그 파일에 기록해 두는 것이다. 데이타의 무결성이 침해되었을 경우, 로그 파일에서 허기되지 않은 접근 시도에 관한 정보를 검토하므로서 무결성 침해의 원인을 쉽게 추적할 수 있다.

세번째 형태의 로그 파일은 하드웨어에 발생한 장애에 관한 정보이다. 예를 들어 시스템 메모리에 장애가 발생하였을 경우, 장애 내용을 로그 파일에 기록해 둠으로서 추후 로그 파일에 기록된 정보를 통해 메모리에 발생한 장애를 해결할 수 있다.

네번째 형태의 로그 파일은 사용자가 정의한 활동을 기록하는 것이다. 이러한 기능은 시스템 보안감사 담당자가 감사 증거 수집 기능을 로깅 기능내에 정의해 둘 수 있어 매우 유리하다. 즉, 응용 프로그램들이 실행될 때마다 로깅 기능에 정의된 정보들이 로그 파일에 자동으로 기록되게 할 수 있다.

5. 결 론

본 연구는 논리적 보안 통제에서 기본적으로 필요한 통제를 식별하고 설명하였다. 기본적으로 필요한 통제를 식별과 인증, 접근통제, 감사로그로 제시하고 각각의 기능에 대하여 설명하였다. 식별과 인증에서는 패스워드, 토큰, 생체측정의 방법을 설명하였다. 식별과인증에서는 어느 한가지 방법에만 국한되어 사용하는 것보다는 혼합하여 사용하는 방법이 효과적이다. 예를 들면 일회용 패스워드와 스마트 카드를 결합하여 사용하는 방법은 패스워드 시스템만 사용하는 것보다는 훨씬 효과적이다.

접근통제에서는 전통적으로 많이 사용되는 임의적 접근통제나 강제적 접근통제을 소개했다. 임의적 접근통제는 보안성 요구가 약한 시스템에 적합하며, 반면에 강제적 접근통제는 보안성 요구가 강한 시스템에 적합하다.

따라서 대부분의 상용 및 일반행정 시스템은 임의적 접근통제 방법에 의존을 많이 하나, 현재의 임의적 접근통제는 많은 취약성을 내포하고 있다. 반면에 강제적 접근통제는 보안성이 뛰어나나 사용하기 불편하며 비용이 비싸다. 최근 많이 연구되고 있는 역할에 따른 접근통제 방법은 임의적 접근통제 보다는 보안성이 뛰어나고, 사용의 불편성이 강제적 접근 방법보다는 적다. 현재 역할에 따른 접근통제에 대한 연구와 표준화가 활발한 이유가 여기에 있으며, 우리 역시 많은 관심을 갖고 연구개발하여야 할 것이다.

마지막으로 감사로그를 논리적 보안통제로 제시하였다. 감사로그는 ISO 7498-2에서는 보안서비스로서 채택되지 않았으나, 현실적으로는 중요한 논리적 통제로 보인다. 최근 감사로그는 사후에 보안사고 분석과 같은 활동에만 사용되는 것이 아니라, 실시간으로 침입자를 탐색할 수 있는 등 그 기능이 점점 확대되고 있다. 이와 같은 보안 서비스에도 많은 관심과 연구가 필요할 것이다.

참 고 문 헌

[1] ISO 7498-2, "Information processing systems-Open Systems Interconnection-Basic Reference Model-Part 2: Security Architeture", 1989.

[2] 한국전산원, "전산망 보안관리를 위한 지침서-소프트웨어 보안", 1994. 12

[3] Computer & Security, Vol.14, No.3, "Biometrics, Is it a Viable Proposition for Identity Authentication and Access Control?", 1995

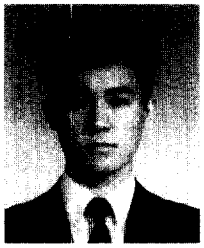
[4] Computer & Security, Vol.9, No.4, "Computer Access Control Policy Choices", 1990

[5] Computer & Security, Vol.12, No.1, "The Role of Roles", 1993

[6] David Ferraiolo and Richard Kuhn, "Role-Based Access Control", 15th National Computer Security Conference, 1992. 10

[7] Ravi S. Sandha and Hal Feinstein, "A Three Tier Architecture for Role-Based Access Control", 17th National Computer Security Conference, 1994. 10

□ 著者紹介



최 운 식(崔雲植, Woosik Choi)

1993년 경북대학교 무기재료공학과 학사
현재 한국전산원 연구원

※ 관심분야 : 정보 보안

신 동 익(申東翊, Dongik Shin)

1978년 고려대학교 식품공학과 학사
1984년 오하이오대학교 경영학과 석사
1991년 네브라스카대학교 경영학과 경영정보학 박사
현재 한국전산원 책임연구원

※ 관심분야 : 정보 보안, 정보시스템 감사, 소프트웨어 공학